Welcome to Cert007 - Your Ultimate IT Certification Partner

- Real Exam Questions
- Free Updates
- Expert Support
- Instant Access
- Money-Back Guarantee

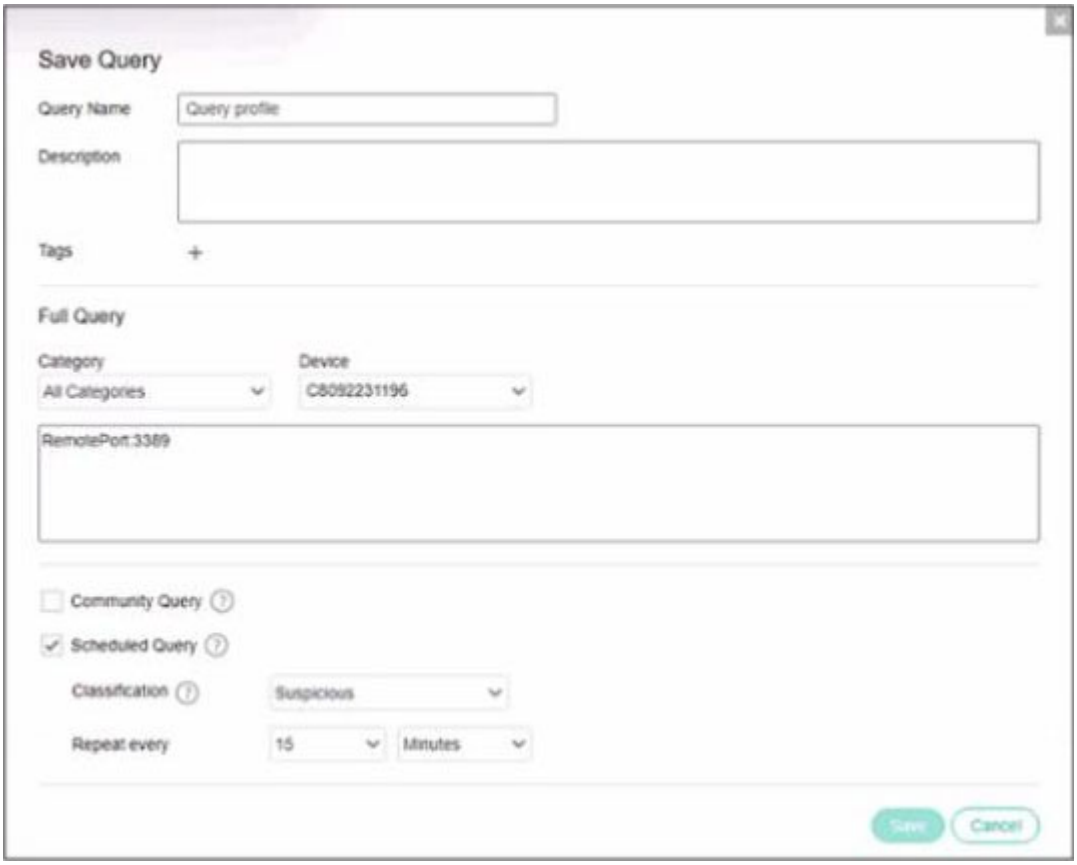
Visit us at **https://www.cert007.com/** for more information

Exam : **NSE5_EDR-5.0**

Title : Fortinet NSE 5 - FortiEDR 5.0 Exam

Version : DEMO

1.Refer to the exhibit.



Based on the threat hunting query shown in the exhibit which of the following is true?

A. RDP connections will be blocked and classified as suspicious

B. A security event will be triggered when the device attempts a RDP connection

C. This query is included in other organizations

D. The query will only check for network category

Answer: B

2.What is the purpose of the Threat Hunting feature?

A. Delete any file from any collector in the organization

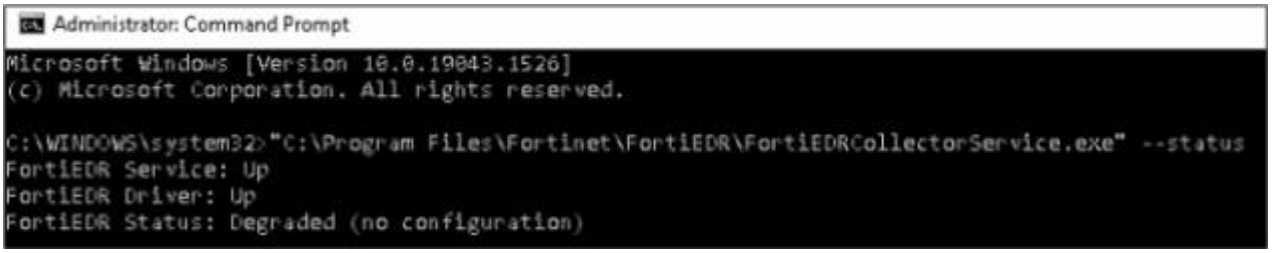
B. Find and delete all instances of a known malicious file or hash in the organization

C. Identify all instances of a known malicious file or hash and notify affected users

D. Execute playbooks to isolate affected collectors in the organization

Answer: C

3.Refer to the exhibit.



Based on the FortiEDR status output shown in the exhibit, which two statements about the FortiEDR

collector are true? (Choose two.)

A. The collector device has windows firewall enabled

B. The collector has been installed with an incorrect port number

C. The collector has been installed with an incorrect registration password

D. The collector device cannot reach the central manager

Answer: B,C

4.Exhibit.

Based on the forensics data shown in the exhibit which two statements are true? (Choose two.)

A. The device cannot be remediated

B. The event was blocked because the certificate is unsigned

C. Device C8092231196 has been isolated

D. The execution prevention policy has blocked this event.

Answer: A D

5.Exhibit.

Based on the forensics data shown in the exhibit, which two statements are true? (Choose two.)

A. An exception has been created for this event

B. The forensics data is displayed m the stacks view

C. The device has been isolated

D. The exfiltration prevention policy has blocked this event

Answer: B C